IMPLEMENTASI INTRUSION PREVENTION SYSTEM MENGGUNAKAN SURICATA UNTUK KEAMANAN SERVER UNIVERSITAS TELKOM SURABAYA MELALUI DETEKSI ANOMALI TRAFIK

IMPLEMENTATION OF INTRUSION PREVENTION SYSTEM USING SURICATA FOR SERVER SECURITY OF TELKOM UNIVERSITY SURABAYA THROUGH TRAFFIC ANOMALY DETECTION

Naufal Rizki Hariyono[1], Oktavia Ayu Permata, S.T., M.T.[2], Rizky Fenaldo Maulana S.Kom., M.Kom.[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Surabaya
[1]naufalrizki@students.telkomuniversity.ac.id, [2]oktapermata@telkomuniversity.ac.id,
[3]rizkyfenaldo@telkomuniversity.ac.id

Abstrak

Serangan siber seperti *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS) sering mengancam operasional institusi akademik. Sistem keamanan konvensional sering tidak efektif dalam mendeteksi dan menanggulangi serangan berskala besar. Oleh karena itu, peningkatan kemampuan deteksi dan pencegahan serangan siber menjadi prioritas utama, terutama di lingkungan akademik yang menyimpan data sensitif.

Penelitian ini menerapkan Suricata sebagai *Intrusion Prevention System* (IPS) untuk mendeteksi dan mencegah anomali serangan pada server Universitas Telkom Surabaya. Suricata memantau lalu lintas jaringan secara real-time dan menggunakan aturan untuk mengidentifikasi serta otomatis memblokir lalu lintas mencurigakan. Integrasi dengan Telegram memungkinkan notifikasi cepat kepada administrator jaringan, sehingga dapat segera mengambil Tindakan tambahan.

Hasil penelitian menunjukkan Suricata IPS efektif dalam mendeteksi dan memblokir paket TCP, UDP, dan ICMP dengan akurasi 99%, meskipun akurasi pada protokol HTTP menurun menjadi 90%. Sistem notifikasi Telegram berhasil memberikan notifikasi real-time dengan delay 1 sampai 2 detik, meski menggunakan sumber daya lebih tinggi. Secara keseluruhan, kombinasi Suricata dan notifikasi Telegram terbukti efektif dalam meningkatkan keamanan server dan mengurangi risiko serangan siber.

Kata kunci : suricata, intrusion prevention system (IPS), keamanan server, serangan siber, anomali